
An Improvement to the Domain Adaptation Bound in a PAC-Bayesian context

Pascal Germain
IFT-GLO, Université Laval
Québec (QC), Canada
pascal.germain@ift.ulaval.ca

Amaury Habrard
LaHC, UMR CNRS 5516
Univ. of St-Etienne, France
amaury.habrard@univ-st-etienne.fr

François Laviolette
IFT-GLO, Université Laval
Québec (QC), Canada
francois.laviolette@ift.ulaval.ca

Emilie Morvant
LaHC, UMR CNRS 5516
Univ. of St-Etienne, France
emilie.morvant@univ-st-etienne.fr

Abstract

This paper provides a theoretical analysis of domain adaptation based on the PAC-Bayesian theory. We propose an improvement of the previous domain adaptation bound obtained by Germain et al. [1] in two ways. We first give another generalization bound tighter and easier to interpret. Moreover, we provide a new analysis of the constant term appearing in the bound that can be of high interest for developing new algorithmic solutions.

1 Introduction

Domain adaptation (DA) arises when the distribution generating the target data differs from the one from which the source learning has been generated from. Classical theoretical analyses of domain adaptation propose some generalization bounds over the expected risk of a classifier belonging to a hypothesis class \mathcal{H} over the target domain [2, 3, 4]. Recently, Germain et al. have given a generalization bound expressed as an averaging over the classifiers in \mathcal{H} using the PAC-Bayesian theory [1]. In this paper, we derive a new PAC-Bayesian domain adaptation bound that improves the previous result of [1]. Moreover, we provide an analysis of the constant term appearing in the bound opening the door to design new algorithms able to control this term. The paper is organized as follows. We introduce the classical PAC-Bayesian theory in Section 2. We present the domain adaptation bound obtained in [1] in Section 3. Section 4 presents our new results.

2 PAC-Bayesian Setting in Supervised Learning

In the non adaptive setting, the PAC-Bayesian theory [5] offers generalization bounds (and algorithms) for weighted majority votes over a set of functions, called voters. Let $X \subseteq \mathbb{R}^d$ be the input space of dimension d and $Y = \{-1, +1\}$ be the output space. A domain P_s is an unknown distribution over $X \times Y$. The marginal distribution of P_s over X is denoted by D_s . Let \mathcal{H} be a set of n voters such that: $\forall h \in \mathcal{H}, h : X \rightarrow Y$, and let π be a prior on \mathcal{H} . A *prior* is a probability distribution on \mathcal{H} that “models” some *a priori* knowledge on quality of the voters of \mathcal{H} .

Then, given a learning sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^{m_s}$, drawn independently and identically distributed (*i.i.d.*) according to the distribution P_s , the aim of the PAC-Bayesian learner is to find a posterior distribution ρ leading to a ρ -weighted majority vote B_ρ over \mathcal{H} that has the lowest possible expected risk, *i.e.*, the lowest probability of making an error on future examples drawn from D_s . More precisely, the vote B_ρ and its true and empirical risks are defined as follows.

Definition 1. Let \mathcal{H} be a set of voters. Let ρ be a distribution over \mathcal{H} . The ρ -weighted majority vote B_ρ (sometimes called the Bayes classifier) is:

$$\forall \mathbf{x} \in X, \quad B_\rho(\mathbf{x}) \stackrel{\text{def}}{=} \text{sign} \left[\mathbf{E}_{h \sim \rho} h(\mathbf{x}) \right].$$

The true risk of B_ρ on a domain P_s and its empirical risk on a m_s -sample S are respectively:

$$R_{P_s}(B_\rho) \stackrel{\text{def}}{=} \mathbf{E}_{(\mathbf{x}_i, y_i) \sim P_s} \mathbf{I}[B_\rho(\mathbf{x}_i) \neq y_i], \quad \text{and} \quad R_S(B_\rho) \stackrel{\text{def}}{=} \frac{1}{m_s} \sum_{i=1}^{m_s} \mathbf{I}[B_\rho(\mathbf{x}_i) \neq y_i].$$

where $\mathbf{I}[a \neq b]$ is the 0-1 loss function returning 1 if $a \neq b$ and 0 otherwise. Usual PAC-Bayesian analyses [5, 6, 7, 8, 9] do not directly focus on the risk of B_ρ , but bound the risk of the closely related stochastic Gibbs classifier G_ρ . It predicts the label of an example \mathbf{x} by first drawing a classifier h from \mathcal{H} according to ρ , and then it returns $h(\mathbf{x})$. Thus, the true risk and the empirical on a m_s -sample S of G_ρ correspond to the expectation of the risks over \mathcal{H} according to ρ :

$$R_{P_s}(G_\rho) \stackrel{\text{def}}{=} \mathbf{E}_{h \sim \rho} R_{P_s}(h) = \mathbf{E}_{(\mathbf{x}_i, y_i) \sim P_s} \mathbf{E}_{h \sim \rho} \mathbf{I}[h(\mathbf{x}_i) \neq y_i],$$

$$\text{and } R_S(G_\rho) \stackrel{\text{def}}{=} \mathbf{E}_{h \sim \rho} R_S(h) = \frac{1}{m_s} \sum_{i=1}^{m_s} \mathbf{E}_{h \sim \rho} \mathbf{I}[h(\mathbf{x}_i) \neq y_i].$$

Note that it is well-known in the PAC-Bayesian literature that the risk of the deterministic classifier B_ρ and the risk of the stochastic classifier G_ρ are related by $R_{P_s}(B_\rho) \leq 2R_{P_s}(G_\rho)$.

3 PAC-Bayesian Domain Adaptation of the Gibbs classifier

Throughout the rest of this paper, we consider the PAC-Bayesian DA setting introduced by Germain et al. [1]. The main difference between supervised learning and DA is that we have two different domains over $X \times Y$: the source domain P_s and the target domain P_t (D_s and D_t are the respective marginals over X). The aim is then to learn a good model on the target domain P_t knowing that we only have label information from the source domain P_s . Concretely, in the setting described in [1], we have a labeled source sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^{m_s}$, drawn *i.i.d.* from P_s and a target unlabeled sample $T = \{\mathbf{x}_j\}_{j=1}^{m_t}$, drawn *i.i.d.* from D_t . One thus desires to learn from S and T a weighted majority vote with the lowest possible expected risk on the target domain $R_{P_t}(B_\rho)$, *i.e.*, with good generalization guarantees on P_t . Recalling that usual PAC-Bayesian generalization bound study the risk of the Gibbs classifier, Germain et al. [1] have done an analysis of its target risk $R_{P_t}(G_\rho)$, which also relies on the notion of *disagreement* between the voters:

$$R_D(h, h') \stackrel{\text{def}}{=} \mathbf{E}_{\mathbf{x} \sim D} \mathbf{I}[h(\mathbf{x}) \neq h'(\mathbf{x})]. \quad (1)$$

Their main result is the following theorem.

Theorem 1 (Theorem 4 of [1]). *Let \mathcal{H} be a set of voters. For every distribution ρ over \mathcal{H} , we have:*

$$R_{P_t}(G_\rho) \leq R_{P_s}(G_\rho) + \text{dis}_\rho(D_s, D_t) + \lambda_{\rho, \rho_T^*}, \quad (2)$$

where $\text{dis}_\rho(D_s, D_t)$ is the domain disagreement between the marginals D_s and D_t ,

$$\text{dis}_\rho(D_s, D_t) \stackrel{\text{def}}{=} \left| \mathbf{E}_{(h, h') \sim \rho^2} (R_{D_s}(h, h') - R_{D_t}(h, h')) \right|, \quad (3)$$

with $\rho^2(h, h') = \rho(h) \times \rho(h')$, and $\lambda_{\rho, \rho_T^*} = R_{P_t}(G_{\rho_T^*}) + R_{D_t}(G_\rho, G_{\rho_T^*}) + R_{D_s}(G_\rho, G_{\rho_T^*})$, where $\rho_T^* = \arg\min_\rho R_{P_t}(G_\rho)$ is the best distribution on the target domain.

Note that this bound reflects the usual philosophy in DA: It is well known that a favorable situation for DA arrives when the divergence between the domains is small while achieving good source performance [2, 3, 4]. Germain et al. [1] have then derived a first promising algorithm called PBDA for minimizing this trade-off between source risk and domain disagreement.

Note that Germain et al. [1] also showed that, for a given hypothesis class \mathcal{H} , the domain disagreement of Equation (3) is always smaller than the $\mathcal{H}\Delta\mathcal{H}$ -distance of Ben-David et al. [2, 3] defined by $\frac{1}{2} \sup_{(h, h') \in \mathcal{H}^2} |R_{D_t}(h, h') - R_{D_s}(h, h')|$.

4 New Results

4.1 Improvement of Theorem 1

First, we introduce the notion of *expected joint error* of a pair of classifiers (h, h') drawn according to the distribution ρ , defined as

$$e_{P_s}(G_\rho, G_\rho) \stackrel{\text{def}}{=} \mathbf{E}_{(h, h') \sim \rho^2} \mathbf{E}_{(\mathbf{x}, y) \sim P_s} \mathbf{I}[h(\mathbf{x}) \neq y] \times \mathbf{I}[h'(\mathbf{x}) \neq y]. \quad (4)$$

Thm 2 below relies on the domain disagreement of Eq. (1), and on *expected joint error* of Eq. (4).

Theorem 2. *Let \mathcal{H} be a hypothesis class. We have*

$$\forall \rho \text{ on } \mathcal{H}, \quad R_{P_t}(G_\rho) \leq R_{P_s}(G_\rho) + \frac{1}{2} \text{dis}_\rho(D_s, D_t) + \lambda_\rho, \quad (5)$$

where λ_ρ is the deviation between the expected joint errors of G_ρ on the target and source domains:

$$\lambda_\rho \stackrel{\text{def}}{=} \left| e_{P_t}(G_\rho, G_\rho) - e_{P_s}(G_\rho, G_\rho) \right|.$$

Proof. First, note that for any distribution P on $X \times Y$, with marginal distribution D on X , we have

$$R_P(G_\rho) = \frac{1}{2} R_D(G_\rho, G_\rho) + e_P(G_\rho, G_\rho),$$

$$\begin{aligned} \text{as } 2 R_P(G_\rho) &= \mathbf{E}_{(h, h') \sim \rho^2} \mathbf{E}_{(\mathbf{x}, y) \sim P} \left(\mathbf{I}[h(\mathbf{x}) \neq y] + \mathbf{I}[h'(\mathbf{x}) \neq y] \right) \\ &= \mathbf{E}_{(h, h') \sim \rho^2} \mathbf{E}_{(\mathbf{x}, y) \sim P} \left(1 \times \mathbf{I}[h(\mathbf{x}) \neq h'(\mathbf{x})] + 2 \times \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] \right) \\ &= R_D(G_\rho, G_\rho) + 2 \times e_P(G_\rho, G_\rho). \end{aligned}$$

Therefore,

$$\begin{aligned} R_{P_t}(G_\rho) - R_{P_s}(G_\rho) &= \frac{1}{2} \left(R_{D_t}(G_\rho, G_\rho) - R_{D_s}(G_\rho, G_\rho) \right) + \left(e_{P_t}(G_\rho, G_\rho) - e_{P_s}(G_\rho, G_\rho) \right) \\ &\leq \frac{1}{2} \left| R_{D_t}(G_\rho, G_\rho) - R_{D_s}(G_\rho, G_\rho) \right| + \left| e_{P_t}(G_\rho, G_\rho) - e_{P_s}(G_\rho, G_\rho) \right| \\ &= \frac{1}{2} \text{dis}_\rho(D_s, D_t) + \lambda_\rho. \quad \square \end{aligned}$$

The improvement of Theorem 2 over Theorem 1 relies on two main points. On the one hand, our new result contains only the half of $\text{dis}_\rho(D_s, D_t)$. On the other hand, contrary to λ_{ρ, ρ_T^*} of Eq. (2), the term λ_ρ of Eq. (5) does not depend anymore on the best ρ_T^* on the target domain. This implies that our new bound is not degenerated when the two distributions P_s and P_t are equal (or very close). Conversely, when $P_s = P_t$, the bound of Theorem 1 gives

$$R_{P_t}(G_\rho) \leq R_{P_t}(G_\rho) + R_{P_t}(G_{\rho_T^*}) + 2R_{D_t}(G_\rho, G_{\rho_T^*}),$$

which is at least $2R_{P_t}(G_{\rho_T^*})$. Moreover, the term $2R_{D_t}(G_\rho, G_{\rho_T^*})$ is greater than zero for any ρ when the support of ρ and ρ_T^* in \mathcal{H} is constituted of at least two different classifiers.

4.2 A New PAC-Bayesian Bound

Note that the improvements introduced by Theorem 2 do not change the form and the philosophy of the PAC-Bayesian theorems previously presented by Germain et al. [1]. Indeed, following the same proof technique, we obtain the following PAC-Bayesian domain adaption bound.

Theorem 3. *For any domains P_s and P_t (resp. with marginals D_s and D_t) over $X \times Y$, any set of hypothesis \mathcal{H} , any prior distribution π over \mathcal{H} , any $\delta \in (0, 1]$, any real numbers $\alpha > 0$ and $c > 0$, with a probability at least $1 - \delta$ over the choice of $S \times T \sim (P_s \times D_T)^m$, for every posterior distribution ρ on \mathcal{H} , we have*

$$R_{P_t}(G_\rho) \leq c' R_S(G_\rho) + \alpha' \frac{1}{2} \text{dis}_\rho(S, T) + \left(\frac{c'}{c} + \frac{\alpha'}{\alpha} \right) \frac{\text{KL}(\rho \| \pi) + \ln \frac{3}{\delta}}{m} + \lambda_\rho + \frac{1}{2}(\alpha' - 1),$$

where λ_ρ is defined by Eq. (6), and where $c' \stackrel{\text{def}}{=} \frac{c}{1 - e^{-c}}$, and $\alpha' \stackrel{\text{def}}{=} \frac{2\alpha}{1 - e^{-2\alpha}}$.

4.3 On the Estimation of the Unknown Term λ_ρ

The next proposition gives an upper bound on the term λ_ρ of Theorems 2 and 3.

Proposition 4. *Let \mathcal{H} be the hypothesis space. If we suppose that P_s and P_t share the same support, then*

$$\forall \rho \text{ on } \mathcal{H}, \lambda_\rho \leq \sqrt{\chi^2(P_t \| P_s) e_{P_s}(G_\rho, G_\rho)},$$

where $e_{P_s}(G_\rho, G_\rho)$ is the expected joint error on the source distribution, as defined by Eq. (4), and $\chi^2(P_t \| P_s)$ is the chi-squared divergence between the target and the source distributions.

Proof. Supposing that P_t and P_s have the same support, then we can upper bound λ_ρ using Cauchy-Schwarz inequality to obtain line 4 from line 3.

$$\begin{aligned} \lambda_\rho &= \left| \mathbf{E}_{(h, h') \sim \rho^2} \left[\mathbf{E}_{(\mathbf{x}, y) \sim P_t} \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] - \mathbf{E}_{(\mathbf{x}, y) \sim P_s} \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] \right] \right| \\ &= \left| \mathbf{E}_{(h, h') \sim \rho^2} \left[\mathbf{E}_{(\mathbf{x}, y) \sim P_s} \frac{P_t(\mathbf{x}, y)}{P_s(\mathbf{x}, y)} \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] - \mathbf{E}_{(\mathbf{x}, y) \sim P_s} \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] \right] \right| \\ &= \left| \mathbf{E}_{(h, h') \sim \rho^2} \mathbf{E}_{(\mathbf{x}, y) \sim P_s} \left(\frac{P_t(\mathbf{x}, y)}{P_s(\mathbf{x}, y)} - 1 \right) \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] \right| \\ &\leq \sqrt{\mathbf{E}_{(\mathbf{x}, y) \sim P_s} \left(\frac{P_t(\mathbf{x}, y)}{P_s(\mathbf{x}, y)} - 1 \right)^2} \times \sqrt{\mathbf{E}_{(h, h') \sim \rho^2} \mathbf{E}_{(\mathbf{x}, y) \sim P_s} (\mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y])^2} \\ &\leq \sqrt{\mathbf{E}_{(\mathbf{x}, y) \sim P_s} \left(\frac{P_t(\mathbf{x}, y)}{P_s(\mathbf{x}, y)} - 1 \right)^2} \times \mathbf{E}_{(h, h') \sim \rho^2} \mathbf{E}_{(\mathbf{x}, y) \sim P_s} \mathbf{I}[h(\mathbf{x}) \neq y] \mathbf{I}[h'(\mathbf{x}) \neq y] \\ &= \sqrt{\mathbf{E}_{(\mathbf{x}, y) \sim P_s} \left(\frac{P_t(\mathbf{x}, y)}{P_s(\mathbf{x}, y)} - 1 \right)^2} \times e_{P_s}(G_\rho, G_\rho) = \sqrt{\chi^2(P_t \| P_s) e_{P_s}(G_\rho, G_\rho)}. \quad \square \end{aligned}$$

This result indicates that λ_ρ can be controlled by the term e_{P_s} , which can be estimated from samples, and the chi-squared divergence between the two distributions that we could try to estimate in an unsupervised way or, maybe more appropriately, use as a constant to tune, expressing a tradeoff between the two distributions. This opens the door to derive new learning algorithms for domain adaptation with the hope of controlling in part some negative transfer.

References

- [1] P. Germain, A. Habrard, F. Laviolette, and E. Morvant. A PAC-Bayesian approach for domain adaptation with specialization to linear classifiers. In *ICML*, pages 738–746, 2013.
- [2] S. Ben-David, J. Blitzer, K. Crammer, and F. Pereira. Analysis of representations for domain adaptation. In *Advances in Neural Information Processing Systems*, pages 137–144, 2006.
- [3] S. Ben-David, J. Blitzer, K. Crammer, A. Kulesza, F. Pereira, and J.W. Vaughan. A theory of learning from different domains. *Machine Learning*, 79(1-2):151–175, 2010.
- [4] Y. Mansour, M. Mohri, and A. Rostamizadeh. Domain adaptation: Learning bounds and algorithms. In *Conference on Learning Theory*, pages 19–30, 2009.
- [5] D. A. McAllester. Some PAC-Bayesian theorems. *Machine Learning*, 37:355–363, 1999.
- [6] D. McAllester. PAC-Bayesian stochastic model selection. *Machine Learning*, 51:5–21, 2003.
- [7] M. Seeger. PAC-Bayesian generalization bounds for gaussian processes. *Journal of Machine Learning Research*, 3:233–269, 2002.
- [8] O. Catoni. *PAC-Bayesian supervised classification: the thermodynamics of statistical learning*, volume 56. Inst. of Mathematical Statistic, 2007.
- [9] P. Germain, A. Lacasse, F. Laviolette, and M. Marchand. PAC-Bayesian learning of linear classifiers. In *International Conference on Machine Learning*, 2009.